

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

THE PREMISES LOCATED AT: 10249 Julius Northway, St. Louis,
Missouri, 63127 located in the Eastern District of Missouri.

Case No. 4:21 MJ 6083 PLC

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Daniel Root, a federal law enforcement officer or an attorney for the government,
request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or
property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed (identify the
person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 USC § 2251 (Production of Child Pornography / Sexual Exploitation) and
18 USC § 2252A (Possession, Receipt, or Distribution of Child Pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing
is true and correct.



Applicant's signature

Daniel Root, Special Agent

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures
4.1 and 41.

Date: 04/29/2021

Patricia L. Cohen

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT: 10249) No. 4:21 MJ 6083 PLC
Julius Northway, St. Louis, Missouri, 63127)
located in the Eastern District of Missouri.) SIGNED AND SUBMITTED TO THE
) COURT FOR FILING BY RELIABLE
) ELECTRONIC MEANS
)
) FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel Root, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), St. Louis Division, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 10249 Julius Northway, St. Louis, Missouri, (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent of the FBI since 2016 and am currently assigned to the FBI St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, post Academy training, and everyday work related to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (Production of Child Pornography / Sexual Exploitation) and 18 U.S.C. § 2252A (Possession, Receipt, or Distribution of Child Pornography) (referred to as “TARGET OFFENSES”) have been committed by **Michael Ulsas** (“**ULSAS**”) or other persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched (the “SUBJECT PREMISES”) is 10249 Julius Northway, St. Louis, Missouri, which is identified as follows: The single-family dwelling numbered “10249” located on the north side of Julius Northway, a street located in St. Louis, Missouri. The Subject Premises is further identified in Attachment A.

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit:
- a. The term “minor” means any individual under the age of 18 years. 18 USC § 2256(1).
 - b. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 USC § 2256(2)(A).
 - c. Visual depiction includes undeveloped film and videotape, and data stored on

computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

d. Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).

e. Identifiable minor means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means.

g. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

7. "Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land

line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

PROBABLE CAUSE

8. On or about 2 April 2021, victim KY and her mother appeared in person at the St. Louis Metropolitan Police headquarters to report a sexual assault. KY and her mother reside in California. KY traveled to St. Louis to report a sexual assault to SLMPD Detective Monzell Scott. Subsequently, from April 20 – 25, 2021, I spoke with Detective Scott extensively about the details of this case. Detective Scott provided me with the SLMPD reports he generated from the interviews with the victim. The details of her initial disclosure to law enforcement come from that report and my discussions with Detective Scott.

9. The matters detailed in this affidavit were initially brought to my attention through collaboration between the Canadian Centre for Child Protection (C3P) and the US Department of Justice. C3P was initially contacted by KY’s mother about removal of child sexual abuse material (CSAM) from Facebook. C3P has been in contact with KY and she has provided C3P with numerous documents. In these documents, she details her victimization. KY also spoke via

telephone with C3P to provide further details. Those details were entered into C3P's case management system and subsequently provided to me for review.

10. I reviewed a copy of a sealed affidavit the Program Manager of C3P, Catherine Tabak, provided in case 18-CR-090-JCC [The "Mahoney" case, which will be detailed later in this affidavit]. Details of C3P's involvement in this case are known to me through this affidavit as well as subsequent communication I had with C3P, the case files provided by C3P, and through subsequent conversations I had with KY. C3P has been involved in this matter since February 2020. Details of KY's reporting to C3P are known to me through the aforementioned sealed Affidavit.

11. C3P contacted the U.S. Department of Justice, Criminal Division, Child Exploitation and Obscenity Section (CEOS) on or about 23 April 2020 and has been in communication with CEOS since then regarding the matters detailed in this affidavit. Between 20 and 26 April 2021, I corresponded with C3P and CEOS on this matter.

12. KY was previously a victim in case 18-CR-090-JCC, in the Western District of Washington. In that case, defendant Thomas Mahoney pled guilty to the following federal offenses:

- a. Travel with intent to engage in a sexual act with a minor (3 counts)
- b. Enticement of a minor

In court documents from case 18-CR-090-JCC, KY is referred to by the initials "MV", used to mean "Minor Victim." Through discussions and collaboration with prosecutors, I learned that KY is the individual identified as "MV" in those court documents.

13. In order to determine KY's age at the time of the events described in this affidavit, I contacted FBI offices in California and requested a database search for a driver's license

matching KY's name. FBI Sacramento responded with a copy of KY's driver's license, number Y8471812, which shows a valid Class C non-commercial driver's license issued on 09/25/2018. The date of birth on the license is 06/20/2002. This birthdate matches the birthdate KY provided to the St. Louis Metropolitan Police Department. Inasmuch KY turned 18 years of age on 6/20/2020.

14. C3P program manager Catherine Tabak detailed in her aforementioned affidavit that between February and April 2020, she became aware of a public Facebook group titled "Thomas Mahoney incident related images and videos" (hereinafter referred to as the "Mahoney Facebook group"). Based on my training and experience, I am aware that Facebook users may create "groups" which provide users with a common interest a place to share conversation, media, and links.

15. Tabak detailed in her affidavit that in April 2020, she accessed and reviewed the Mahoney Facebook group. She found the group to have at least five members at the time she reviewed it. Tabak further detailed the content of the group by describing the posts that users made. In an undated post, Tabak observed numerous comments that appeared to discuss the court documents related to the Mahoney case. For example, the Facebook user "Author," which in my training and experience refers to the person who created the group, posted the following comment: "got the docs only page 10 is missing will post later." A subsequent post read "dm me ill send you all the ones I have bro."¹ A Facebook user EB later posted a Dropbox link titled "Mahoney Documents.zip" In the Facebook group, users traded information that was gleaned from public records (i.e. PACER) that revealed details of KY's victimization. Further documents were

¹ Based on my training and experience, I am aware that "dm" is short for "direct message," a Facebook form of text messaging.

acquired that detailed her health providers and traded in the group. Tabak stated in her affidavit that KY and her mother repeatedly reported the offending content to Facebook, who would take down individual posts but did not dismantle any groups or ban any users.

16. With this information, Mahoney group members harassed KY by continuously posting her personal information on Facebook and other online sites as well as and sending her harassing messages.

17. In discussion that KY had with C3P, and later in documentation KY sent to me (as described later in this affidavit), KY indicated that she believed she identified the individual most responsible for the content of the Mahoney Facebook. KY stated that the person used the Facebook display name “Mike Kanashi.”² This user was the most active in the group and appeared to be the one who made the most number of posts.

18. In the documents that KY sent me on 25 April 2021, she stated that Mike ULSAS was friends with Thomas Mahoney through Facebook. She stated that ULSAS posted on Facebook that KY was the reason that Mahoney was in jail, and that she should “get what she deserves.” ULSAS also encouraged other Facebook users to harass KY by disseminating the child sexual assault material (CSAM) that was produced of KY when she was 14 years old.

19. On 25 April 2021, your Affiant spoke with KY via telephone and provided KY a link to a secure FBI information system where she could send further information and upload any supporting documentation, videos, or images. KY sent me two PDF documents with a narrative style explanation of the events that are detailed in this affidavit.

² KY later determined that the Facebook username “Mike Kanashi” was being used by Michael Ulsas, as detailed further in this affidavit.

20. In the document that KY sent me, she stated that members of the Mahoney Facebook Group harassed her and shared child sexual assault material (CSAM) of her, as well as targeted her for more abuse. She stated that she reported matters to various police departments concerning this abuse. She also detailed the effect that the Mahoney Facebook group had on her. She described the steps she took to mitigate the effect, including moving and participating in the California Safe at Home program. She also sought a sealed name change. KY stated that after repeated reports to NCMEC, C3P, and local law enforcement agencies, the harassment and threats only got worse.

21. KY stated that at some point she felt as though she had nothing left and planned to kill herself. She said she wanted to confront “Mike Kanashi” in person to show that she was a real person who had been pushed the point of suicide from his harassment. KY communicated with “Mike Kanashi” via Facebook and told him that she wanted to meet him in person to confront him. He responded, “LOL no, you need help and it’s not going to be from me.”

22. As some point “Mike Kanashi” eventually agreed to meet KY and provided an address where they would meet, 1430 S. Kirkwood Rd. in St. Louis, Missouri, which is a gas station. Thereafter, on or around April 24, 2020 KY traveled from California to St. Louis, Missouri to confront “Mike Kanashi.” KY was under the impression that was his actual name but later, upon meeting him, she learned that his name was in fact Michael ULSAS.

23. ULSAS and KY met in person and KY described his behavior as polite and nothing like he was acting online. ULSAS apologized to KY and stated that the whole ordeal was just a “joke.” He then invited her to “hang out” at a friend’s house. KY stated that she did not get many social invitations to hang out due to her isolation and social difficulties from having autism. As such, she accepted the invitation as she thought she would be safe as it was with a group of people.

24. The details of KY's first encounter with ULSAS in April 2020 were gathered from the document she sent to me on 25 April 2021 as well as a review of the St. Louis Metropolitan Police Detective Scott's interview of KY on or around 4 April 2021.

25. KY said that she and ULSAS both drank alcohol while hanging out at the friend's house. KY indicated that she remembered the address of the house as 3162 Ohio Avenue in St. Louis. KY had not been in any situations before with social drinking and wanted to fit in with the group. She became very intoxicated. KY detailed in the document that she sent me, as well as in the interview with Detective Scott, that ULSAS took her to a bathroom at the residence and forcefully directed to her knees and instructed her to perform oral sex on him, which ULSAS recorded with his phone.

26. KY did not want ULSAS to distribute the photographs that he had taken of the sexual encounter in her inebriated state and as such tried to stay on good terms with him. At the time of this act, KY was 17 years of age.

27. After a brief stay in St. Louis, KY returned to California but maintained contact with ULSAS as she did not want him to distribute the photographs he took. In photographs ULSAS took of KY during this time, he told her to look 'happy' in the pictures.

28. In an e-mail KY wrote to me on 26 April 2021, she stated that she had daily communication with ULSAS after she returned to California and before she visited St. Louis again, later in 2020. She stated that they communicated via Snapchat and that she wanted to communicate with him as much as possible to keep him "close" because she believed she could get ULSAS to view her as a real person and not release the sexual videos he had produced in April 2020. KY stated that she sent nude photographs to him at his request and added captions that she knew he would like to try and play along with him. In the same e-mail, KY stated, "I do admit I lied to him

as much as possible and complied pretending to have enjoyed the night out of fear or more child pornography distribution.”

29. On or about 22 May 2020, KY again traveled to St. Louis in person. The details of this trip are again detailed in the documents that KY sent me on 25 April 2021 as well as in the statements KY made to St. Louis Police Detective Scott.

30. In the May 2020 trip ULSAS picked KY up at the airport with a person KY later learned to be Tim, ULSAS’s cousin. They travelled to Tim’s house at 4616 Adkins Ave. St. Louis, Missouri. Present at the residence were Tim, Tim’s mother, ULSAS, and KY. After Tim and his mother went to sleep, KY stated that ULSAS forcibly raped her. In the statement KY sent me on 25 April 2021, she described the rape:

During this forcible and terrifying rape I clearly communicated that I was going to die and told him this as it was ongoing. I was begging him to stop and saying he was going to kill me. He did not care whatsoever, he just continued beating and choking me regardless of my pleas and struggles until I would go limp and couldn’t speak, move, or communicate. At times I would be able to muster words such as “you’re killing me you need to stop, I can’t breathe”. That would just make him more angry and he would choke me and beat me even harder. Eventually he passed out from intoxication. I was in so much pain I couldn’t walk and had to crawl over to the bed I was supposed to be sleeping on even though it was less than 10 feet away. Once I fell asleep, he woke me up by attempting to rape me again and I pleaded with him to stop. After about 10 minutes of him refusing to stop, I couldn’t stop crying and hyperventilating so he got angry, drank a lot more alcohol, and went back to bed because he couldn’t maintain an erection due to his heavy alcohol use anyway. He took photos and videos throughout this entire violent rape from start to finish. He showed the photos to me in the morning while laughing. I said don’t you realize that’s rape? And he just couldn’t stop laughing. Then he said well, then you shouldn’t have let me drink so much, what did you expect?

31. KY stated that the next day, ULSAS was overly nice, complimented KY incessantly, and told her that he loved her. Due to the violent nature of the rape, KY had bruises, experienced difficulty walking, sitting, and standing for at least a week. KY called her mother and told her she was in a dangerous situation and her mother offered to get her an Uber to the airport.

However, KY had told her mother that she was with a friend in Texas, and as such did not take her up on the offer. KY did not disclose the rape to her mother until 16 July 2020. Later, KY attempted to report the rape to Sunset Hills, Missouri Police, but was told that she had to appear in person to report it.

32. In the documents that KY sent me on 25 April 2021, she included a screen captures of a Snapchat conversation between her and a user with the display name of “Mike.” The username is not visible in the screen capture. In the chat, KY told “Mike” “On May 22, when I was 17, you violently raped me.” She detailed the physical issues she had after that event and stated that she did not consent to what occurred. The user “Mike” responded, “I wanted to have sex with you, it got out of hand.” “I understand I fucked up” “It won’t happen again” “Is that what you want me to say? Sorry for violently raping you? Like yeah dude I’m sorry.” KY replied that she wants a true apology, and “Mike” responded that he was deeply sorry for his action and that the thought doing “that” to her made him sick to his stomach. He stated that he cannot even begin to imagine the horror she went through at his hands. He further stated that he was not proud of what he did.

33. As previously noted in this Affidavit, KY traveled with her mother to St. Louis to report the forcible rape described above. Based on my discussions with SLMPD Detective Scott, I learned that due to KY’s reports, St. Louis City Police initiated an investigation of ULSAS for sexual abuse. As part of that investigation, on or around 12 April 2021, ULSAS appeared at the St. Louis Metropolitan Police Department for questioning in reference to the sexual assault reported by KY. I was provided a video recording of the interview. Through my conversations with Detective Scott and review of the interview, I learned the details of ULSAS’s statements to the St. Louis Metropolitan Police Department.

34. When the detective told ULSAS that the investigation concerned allegations of a forcible rape of KY, ULSAS told Detective Scott that the interaction was consensual. To substantiate his claim, ULSAS produced his phone and showed Detective Scott a video of a sexual encounter between ULSAS and KY. ULSAS admitted to the Detective it was him and KY. ULSAS chose a video to display to the Detective that occurred when KY had reached the age of 18. With ULSAS's consent, Detective Scott connected ULSAS's cellular telephone to a SLMPD computer. He transferred videos and images from ULSAS's "camera roll" to a computer. The data transferred totaled over 14 GB, and contained over 6,000 files. Due to the volume of data, the videos and photographs were not fully analyzed until after ULSAS left the interview. Detective Scott provided the FBI St. Louis Division with the media he had transferred from ULSAS's phone. He did not alter or edit the data in any way.

35. I reviewed files that were located on ULSAS's phone and transferred to the SLMPD computer. One such image had a filename of IMG_20200523_004940-01.jpg. Based on my training and experience, this filename is consistent with smartphone naming conventions and would indicate that the photograph was taken on or around 23 May 2020. In addition to the filename, I am aware that most smartphone embed metadata in photographs and videos that indicate information such as the time and date taken, the model of phone used, GPS location, and other information. I reviewed the metadata in the image which showed the date taken as 23 May 2020. This is consistent with the filename indicating the date taken of 23 May 2020.

36. The photograph depicts a hand around the throat of a female who I recognize as KY. KY appears topless in the photograph. The photograph contains metadata indicating it was taken at GPS coordinates 38.582410, -90.262140. These coordinates resolve to 4616 Adkins Ave. in St. Louis, MO, the location where KY reported that the sexual abuse occurred. The metadata

and filename of this image that was located on ULSAS's phone is consistent with the details of the events that KY provided to both me and SLMPD Detective Scott.

37. Over the following months, ULSAS continued to interact with KY via Snapchat when she was back at her home in California. In her written statement she sent to me on 25 April 2021, she stated:

With autism and severe PTSD, when I would have a rough day instead of Michael helping to comfort me, he'd encourage me to cut myself and send photos. He wanted me to carve his name into my skin because he "gets off on it". And clearly I wouldn't be in the right state of mind during those times, also I would be on my prescription benzodiazepines (for panic attacks) so I couldn't make good decisions... and I'd oblige. By this point he was the only person who had talked to me in months and he was the only person in my life. I felt like I had to do everything he said due to prolonged psychological manipulation.

38. Based on later review of the media copied from ULSAS's phone, I viewed numerous videos and photos that clearly depict ULSAS and KY engaged in various sexual acts which did occur after she had reached the age of 18. Also located in the data obtained from ULSAS's mobile phone was a video with filename 20200529_094021.mp4. This video is a 1 minute and 51 second video that depicts a male who appears to be ULSAS digitally penetrating the vagina of a female who, based on KY's reports and the facts of the case is KY, although KY's face is not visible in the video. A brief image the male is visible when the phone's camera is pointed at a mirror in a hotel room. The physical characteristics are consistent with my knowledge of ULSAS's appearance, especially when compared with other images of ULSAS that were located on his phone around the time of the creation of the video. The male in the video is wearing a black shirt. In other photographs and videos on obtained from the phone ULSAS is clearly visible and identifiable, wearing a black shirt

39. To authenticate the video, I called KY on 25 April 2021 as mentioned earlier in this Affidavit. This was the first direct contact that FBI St. Louis had with KY. I prepared a number

of redacted images from the video 20200529_094021.mp4 which were obtained from ULSAS's mobile phone. Without discussing any details of the case, I asked if KY would be willing to receive the photographs and identify what they were. KY agreed and consented for the interaction to be audio recorded by me. I sent a low-resolution close-up photograph of a foot in a green sock. KY immediately stated that the photograph was a picture of her foot from a "pornographic video" that ULSAS had made of her at the Pear Tree Inn in Fenton, Missouri. Due to the immediate recognition of the still frame, I did not send any further images to KY.

40. During the conversation with KY, she stated that she actually had a copy of the video that ULSAS sent her - as proof that he maintained the video - in furtherance of his threats to release it should she not comply with his demands. As directed by me, KY uploaded the video to a secure FBI system and I reviewed it. It was the same video as 20200529_094021.mp4 previously referenced. As previously described in this Affidavit, I am aware that most digital cameras and smartphones embed metadata in videos and photographs when they are created. This metadata can include the date and time of creation, GPS location data, and information about the device that created the image. I reviewed the metadata from the file 20200529_094021.mp4. Embedded in the file was metadata showing that the video was taken on 05/29/2020. This is consistent with the filename which indicates the same date, as well as corroborates the information provided by KY.

41. KY stated she had another video that was taken at the Pear Tree Inn, at the same time, which she also uploaded to the secure FBI system. I reviewed this video. I did not recognize the video as one that was obtained from ULSAS's phone device and had not previously seen the video. The video, 1 minute and 50 seconds in length, depicts KY being made to perform oral sex on a male. The male's face is not visible. The male is wearing a black shirt. It appears to be filmed in the same hotel room as 20200529_094021.mp4. In the video, the male forcefully thrusts his

penis into KY's mouth. She attempts to stop multiple times, but the male tells her to continue. KY appears to be in distress and crying. Bruises are visible on KY's chest. The male smacks KY on her face and says, "Who fucking owns you?"- and KY says, "Can't do it anymore." KY told me the male was ULSAS.

42. As previously mentioned KY's birthdate is 06/20/2002. She turned 18 years old on 06/20/2020. Therefore, her age at the time that video 20200529_094021.mp4 was created was 17 years old meaning the video depicts a sex act when KY had not reached 18 years of age. Because KY had not yet reached the age of 18, I believe that the video constitutes child pornography as described in 18 USC § 2256.

43. In my conversation with KY on 25 April 2021, KY stated that ULSAS created numerous Facebook accounts because Facebook keeps shutting down his various accounts for violations of the terms of service. KY stated that ULSAS was actively posting on Facebook about his recent encounter with St. Louis Metropolitan Police Department and bragging that he had walked away from the encounter without being arrested.

44. The document KY sent me on 25 April 2021 contains numerous screenshots of posts that KY found relevant. The screenshots were from numerous Facebook and Snapchat accounts that KY stated were used by ULSAS. One screenshot from user with vanity name "Michael Fukdathoe" reads "I love being arrested! Fuck this bitch!!!" and in the comments the same user posts "She's claiming rap [sic] from like April and May of last year." Further in the same thread, a user "Jonah Anderson" commented "She cancelled you, now it's time for you to cancel her existence" "as in murder her, with a premeditated motive." KY said this post made her fear for her life.

45. “Michael Fukdathoe” continued to post in the comments on that thread. For example the user posted, “[t]hey took their time building a case” “Not arrested just detained and questioned” “For like 5 hours.” Additional comments suggested hiring a hitman “to grief her house in Minecraft” which KY believes is a code to cover the concept of actually committing murder-for-hire. ULSAS responded “I can’t afford a Minecraft account,” which KY said indicated that the lack of funds is what was keeping him from hiring someone to murder her.

46. Concerning ULSAS’s mindset towards those who accuse him of sexual offenses, KY included a screenshot of a post made by Facebook user “Mike Kanashi” that read: “[e]ternally laughing my ass off at the face this bitch who tried to press sexual harassment charges on me got hit by a car and died and the charges got dropped.” KY provided numerous additional screenshots from various Facebook accounts. I filed preservation requests with Facebook for all these accounts. While legal process is pending to identify the internet protocol addresses used to access the accounts, I attempted to view each Facebook account. Some were no longer available, but those that were still available had activity that was consistent with one user creating multiple accounts, such as having common friends. Some also had further evidence that they were linked to ULSAS due to the posted content on the Facebook account being found also in the files that Detective Scott extracted from his phone.

47. For example, the Facebook account with vanity name “Mike Luvskatie” and username *mike.luvscok* has a photograph of ULSAS as the profile picture and a post reading: “[t]his is my alternate account, sometimes I like to pretend like a gigantic pussy on the internet and act like I care about women so girls will message me.” Additionally, the account with vanity name “Micheal Lightning” and username *micheal.lightning.39* has a profile video of a young girl saying

“No, you’re black, ugly, nigg-“ before it cuts off. That identical video was on ULSAS’s phone when Detective Scott extracted the video.

48. In addition to the previously described Facebook accounts KY provided extracts of from a variety of other Facebook accounts that she indicated were likely associated with ULSAS. These posts and they are reproduced below:

From Facebook user “Micheal [sic] Lightning”

- a. Lmfao can you imagine how easy it’d be to rape these two walking home at night?
They’d just stop resisting like 2 minutes into it
- b. Okay reddit is it morally wrong to force my ldr girlfriend to get a sugar daddy so she can fund my drug habit because she doesn’t want to start an only fans?
- c. Well she has too much “social anxiety” to get a job and she turned down a lot of 14-18 an hour job cause of Cali’s super high minimum wage and I need money
- d. Really I just want to watch her get paid to shove large object inside herself for my amusement

From Facebook user “Michael Martinez”

- a. Women should not feel safe walking next to me in public
- b. If you have pierced nipples and you wear a skintight white t-shirt that blatantly shows off your nipples don’t get mad at me for following you home at the end of the night, learning your routine, and placing cameras in your house. Reevaluate your life choices
slut

From Facebook user “Mike Mcchikin”

Women deserve nothing but death and that’s a fact

From Facebook user “Michael Notafryguy”

- a. I hate women for existing, the slightest fuck up will send me into an uncontrollable rage and them to the ER
- b. But yeah I'm gonna delete all my accounts before I get put on the sex offender registry lmao, might add some people on a new account or my irl but it won't be Mike kanashi, it'll just be me
- c. Lol the first night she met me I passed out and left her in a car with a stranger showing her his gun

From Facebook user "Mike Luvskatie"

Whenever someone on the internet makes me mad I just punch [KY] in the stomach lol, I think I accidentally cracked her ribs last time.

From Facebook user "Goodguy Mike"

- a. Arrested for drunk and disorderly in the parking lot
- b. I'm on felony probation I won't catch an assault charge but don't fucking try me

From Facebook user "Jason Borges"

- a. Having sex with a 17 year old is a natural antidepressant
- b. I'm sexually harassing every girl I've seen so far today
- c. I can't handle rejection so I have sex with minors because they don't know how to say no
- d. I have sex with children, grow the fuck up
- e. I've raped THREE women tops, I'm not a rapist
- f. I'm a pedophile
- g. Don't add me unless you're a pedophile
- h. I'm not saying I'm a rapist but if a girl finds herself alone in a dark alley and

stumbles across me she better fear for her life

i. I didn't want to post anything about it because I knew I'd lose friends but god my dick is so fucking sore from fucking [KY'S nickname] tiny little mouth with my fat cock
lmaooooo

j. She's a really sweet girl, she just wanted me to stop bullying her lol

49. I served preservation requests and subpoenas to Facebook on 26 April 2021 for all identifiable aforementioned accounts. Facebook responded with subscriber information the same day. The user accounts "Micheal Lightning", "Michael Fuckdathoe", "Mike Luvskatie" and "Micheal Capone" all had their most recent login from IP address 75.132.13.59. A search of FBI databases indicated that IP address 75.132.13.59 is owned by Spectrum Charter. I served a subpoena to Charter on 27 April 2021 and am awaiting results.

50. The recovery e-mails for the given Facebook accounts are as follows:

"Michael Fuckdatho" is mikeykanashisushi@gmail.com.

"Micheal Lightning" is racistpedophile@gmail.com.

"Micheal Capone" is mikekanashisushi@gmail.com.

I served subpoenas to Google for those accounts on 27 April 2021 and am awaiting results.

51. Based on my training and experience, the same IP accessing multiple Facebook accounts is indicative of a user that has created multiple profiles. This information is consistent with information provided by ULSAS to Sunset Hills, Missouri Police, that he creates multiple Facebook profiles. This information is also consistent with information provided by KY me that ULSAS creates multiple fake Facebook profiles.

52. I searched the Missouri Department of Revenue records and located a Missouri driver's license for Michael ULSAS with operator number B200098012. The address listed on the license is 10249 Julius Northway St. Louis, SUBJECT PREMISES.

53. On 19 April 2021, Special Agent Matthew Baughn of the FBI located ULSAS at the SUBJECT PREMISES and interviewed him about comments made on Facebook. During that interview with Special Agent Baughn, ULSAS stated that he lived in the basement of SUBJECT PREMISES. During the interview, Special Agent Baughn noted that ULSAS was being monitored by an ankle monitor.

54. I contacted Sunset Hills Police Department to inquire about ULSAS's monitoring. On 27 April 2021, I received an e-mail from Sunset Hills Police Detective Dan O'Brien. Attached to the e-mail was a Sunset Hill Police report 20-16150. The report details that an employee of a nail salon in Sunset Hills contacted the police reporting that someone had made a comment on Facebook that he "wants to rape and murder a woman working at the" nail salon next door, but the only reason he didn't do so was because he didn't want to lose his job at the Five Guys Burgers restaurant next door. Sunset Hills Police went to 10249 Julius Northway, the SUBJECT PREMISES, and located ULSAS inside. Sunset Hills Police questioned ULSAS about the posts. Initially, ULSAS stated that it was probably his girlfriend, KY, who made the post. When ULSAS and the officer went outside, however, ULSAS admitted that he made the post under a fake Facebook account. ULSAS was shown a Facebook post which read "There's an Asian nail tech who works at the same plaza as me and she's constantly taking trash out by herself and every time she walks past me smoking a cigarette I'm consumed with a murderous lust". ULSAS admitted to being the person who posted that statement. The same Sunset Hills police report detailed that

ULSAS also talked about his girlfriend and stated that he used to bully her for years online, and that she traveled to St. Louis to confront him, and that the two were then engaged in a relationship.

55. ULSAS was arrested for Terroristic Threatening and the case was presented to the St. Louis County Prosecutor's Office, who took it under advisement.

56. On 27 April 2021, I called Kurt Stierwalt with Missouri Probation and Parole. Stierwalt told me that he supervises ULSAS in an out-of-state probation case from Georgia. Stierwalt indicated that ULSAS was driving through Georgia and was pulled over. A search of his car revealed drugs and he was charged. After the incident in Sunset Hills where he made the threatening statements, Stierwalt began monitoring ULSAS via ankle bracelet.

CHARACTERISTICS OF PORNOGRAPHY PARTICIPANTS

57. In addition to participating in child exploitation investigations, your affiant has discussed the aspects of computers and their relationship with child pornography offenses with others. Based upon my knowledge, experience, and communications with other individuals involved in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography.

58. Based on my training and experience, and the training and experience of other agents, I believe that a resident residing at the SUBJECT PREMISES is a collector of child pornography. I base this conclusion on the following facts:

a. Individuals who receive and collect child pornography may receive sexual gratification, stimulation, and satisfaction viewing children engaged in sexual activity, in sexually suggestive poses such as in person, in photographs, other visual media, or from literature

describing such activity. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification;

b. Individuals who receive and collect child pornography do so in a variety of media, including, but not limited to, digital images and videos of child pornography. Based on the evidence obtained in this investigation, **ULSAS** likely possessed child pornography that he produced with a minor.

c. Individuals who receive and collect child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a computer in a private residence, allows the collectors the opportunity to safely maintain their collections for many years and enable the collector to frequently view the collection, which is valued highly. Based on the evidence obtained in this investigation, files of child pornography are likely being stored on electronic devices at a private residence; and

d. Child pornography collectors may also correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit materials; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

59. Based on my training and experience and my conversations with other investigations, child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and

videotapes, at their private residence, for many years. The nature of the materials, their attraction to the materials, and the risk involved with receiving, downloading, and possessing such materials, motivates collectors to keep their child pornography collection within their possession and control wherever they go. Because collectors of child pornography place an extremely high value on their collection, they will take their collection with them if they move from one location to another or else keep it in a secure location nearby.

60. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Here, the target has willingly received images of child pornography. Based on all of the above and my training and experience, your affiant believes that **ULSAS** is a collector of child pornography and that child pornography is likely to be found on one or more of his electronic devices.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

61. In my training and experience, I know that cellular phones (“smart phones”), contain software and hardware that are the same, if not more sophisticated, than a typical home computer. The term “computer,” “hard drive,” and “computer media,” as used in this affidavit, also refers to cellular “smart” phones.

62. I also know that “smartphones” often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a phone that is connected to a desktop or laptop computer, can easily transfer onto other media.

63. A computer’s ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to

as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

64. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

65. Collectors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Kik and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer, even if the user is accessing the information on their cellular "smart phone." Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

66. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the

computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

67. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or

destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

68. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

69. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the TARGET OFFENSES, and thus should all be seized as such.

70. Affiant knows from training and experience that even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Specifically, when a user deletes a file, it goes into a “trash” folder. When the user directs the computer to “empty” the trash folder the contents of the folder, including the deleted file, disappear. However, the file has not left the computer and under normal circumstances, is recoverable by computer experts until it’s overwritten because there is no longer unused space in the computer’s hard drive. How soon a file will be overwritten depends on a number of factors: whether the user is computer savvy and has installed a program that accelerates the normal overwriting of deleted data, how often new files are saved to his hard drive, the capacity of the hard drive, and how the computer’s file system allocates new files. Trained certified computer forensic examiners routinely extract incriminating deleted files from hard drives, usually without difficulty.

71. Since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it (called “slack data”), which are still retrievable because they have not yet been overwritten even if overwriting has begun. Before a file is deleted, the file system marks it as unavailable to be overwritten. Once it is deleted, its data are no longer protected against being overwritten, but the file system won’t necessarily overwrite it all at once, and if it’s only partially overwritten computer experts can recover the portion of the data that has not been overwritten, or at least can match it to images they obtained from, for example, a website, to verify that the images were once in the computer’s hard drive and thus had been possessed. Although a savvy computer user can direct his computer to ensure quick (even instantaneous) overwriting, the default settings on standard operating systems do not do this.

72. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which specific expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

73. The search of computers, hard drives, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will intentionally mislabel directory structures, folder names, and filenames

to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

74. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

SEARCH METHODOLOGY TO BE EMPLOYED

75. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);
- b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data

that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

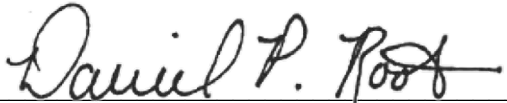
- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or,
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

76. Based on the foregoing I believe there is probable cause that violations of 18 U.S.C. § 2251 (Production of Child Pornography / Sexual Exploitation) and 18 U.S.C. § 2252A (Possession, Receipt, or Distribution of Child Pornography), the previously identified TARGET OFFENSES, have been committed by ULSAS or other persons known and unknown. I also submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B. As described previously in this affidavit there is probable cause to believe that electronic devices, including the mobile phone used by ULSAS, will be located in the SUBJECT PREMISES. The electronic device will contain evidence of the target offenses, including videos and images of child sexual assault material and sexual abuse of KY.

77. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



DANIEL ROOT
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 29 day of April 2021.



PATRICIA L. COHEN
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The location to be searched (the “SUBJECT PREMISES”) known as 10249 Julius Northway, St. Louis, Missouri, which is identified as follows: The single-family dwelling numbered “10249” located on the north side of Julius Northway, a street located in St. Louis, Missouri.



**ATTACHMENT B
LIST OF ITEMS TO BE SEIZED**

All evidence, instrumentalities and contraband concerning the violations of 18 U.S.C. § 2251 (Production of Child Pornography / Sexual Exploitation) and 18 USC § 2252A (Possession, Receipt, or Distribution of Child Pornography) including:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:
 - a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);
 - b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and
 - c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.
4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.
5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.
6. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.